UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF FLORIDA

UNITED STATES OF AMERICA,

Plaintiff,

v.

GREGORY MALCOLM GOOD,
WILLIAM MICHAEL SPEARMAN,
MATTHEW BRANDEN GARRELL, and
ROBERT PRESTON BOYLES

Defendants.

Case No.: 22-CR-80173-AMC

NOTICE OF UNITED STATES' INTENT TO OFFER EVIDENCE UNDER RULES 702, 703, AND 705 & REQUEST FOR RECIPROCAL DISCOVERY

PLEASE TAKE NOTICE that Plaintiff, UNITED STATES OF AMERICA, intends to offer evidence under Rules 702, 703, and 705 of the Federal Rules of Evidence in its case-in-chief at trial in this case.

1. <u>Notice of Evidence Under Rules 702, 703, and 705</u>

Pursuant to Rule 16(a)(1)(G) of the Federal Rules of Criminal Procedure and Southern District of Florida Local Rule 88.10(o)(3)(A), the United States provides this disclosure concerning the potential expert testimony of the following witnesses that the United States may seek to introduce at trial pursuant to Rules 702, 703, and 705 of the Federal Rules of Evidence. The United States also reserves the right to offer additional testimony by these experts, or other expert witnesses, and for the experts to amend or adjust their opinions and bases therefor, based on information perceived by or made known to the experts before or during trial.

a. Jon-Robert Marsh

Jon-Robert Marsh is a Data Scientist with the Federal Bureau of Investigation ("FBI"). He has been in this position since 2021. In this position, he conducts computer forensic extractions and analysis for the Child Exploitation Operational Unit, within the Violent Crimes Section of the FBI's Criminal Investigation Division. In particular, he regularly conducts and assists other investigators with conducting forensic analysis of seized computer systems, servers, mobile devices, and other digital media to provide investigative and analytical support to prosecutors and law enforcement agents. He has conducted and assisted with numerous investigations of offenses involving the online sexual exploitation of children, including over the Tor network and other online networks and services, and regularly assists other FBI investigators with the onsite seizure and examination of digital evidence pursuant to federal search warrants. Prior to his current position, Mr. Marsh worked as an Information Technology Specialist for the FBI from 2010 to 2021, where he likewise conducted computer forensic extractions and analysis and also served as the team leader for a five-member team of computer forensic examiners. Prior to his work with the FBI, Mr. Marsh worked as a Computer Forensic Examiner for the Department of Defense.

Mr. Marsh has numerous certifications, including certifications in Encase, Digital Forensics, and Forensic Computer Examination. In addition to his on-the-job experience analyzing digital devices, he has taken numerous training courses connected to the analysis of computers, mobile devices, and other digital evidence. He also holds a bachelor's degree in Information Systems and Decision Sciences from Louisiana State University in Baton Rouge, Louisiana. A copy of Mr. Marsh's curriculum vitae will be produced in discovery.

In the last four years, Mr. Marsh has testified as an expert witness on one occasion, at a sentencing hearing in the following case: *United States v. Glenn Edward Nutt*, 2:18-CR-00407-

MHT-SRW (M.D. Ala. May 28, 2019). Mr. Marsh has also not authored any publications in the last ten years.

The Extraction of Data from Digital Devices

Although the United States does not believe that testimony regarding the extraction of data from digital devices is expert testimony under the Federal Rules of Evidence,[1] in an abundance of caution the United States is providing notice that, absent a signed stipulation between the parties, it intends to offer testimony from Mr. Marsh regarding the process through which he uses forensic tools to extract and analyze data from seized digital devices.

In particular, after testifying about his training and background discussed above, Mr. Marsh may testify about: the physical inventorying of a digital device, such as a thumb drive or a computer's hard drive, once it is identified during the execution of a warrant and then submitted as an evidence item in an investigation; the creation of a forensic image copy of a digital device after its submission into evidence, including the use of write-blocking technology to protect the integrity of the original evidence item when creating a forensic image copy of it for examination; the generation and use of a hash value associated with a digital device to verify that the working forensic image copy of the device created through the prior steps is an exact match (or "forensic image") of the original evidence item; the purpose behind imaging and hash-matching the original digital evidence item, including to ensure that the original evidence item is not damaged or altered during any subsequent forensic examination and that the forensic image copy being analyzed contains the same data as the original evidence item; and the reliability of the various programs

[1] *See United States v. McLeod*, 755 Fed. Appx. 670, 673-74 (9th Cir. 2019) (unpublished) (district court did not abuse its discretion by admitting testimony without requiring compliance with Rule 702 where witness testified about what Cellebrite does, how he used it to extract information from a cell phone, and how he could select what data to extract); *United States v. Seugasala*, 702 F. App'x 572, 575 (9th Cir. 2017) (unpublished) ("The officers who followed the software prompts from Cellebrite and XRY to obtain data from electronic devices did not present testimony that was based on technical or specialized knowledge that would require expert testimony.")

that he uses to parse, examine, and analyze the matching data contained on the forensic image copy of the digital evidence item.

Mr. Marsh is likewise expected to testify as to how, with respect to the devices that the FBI seized during the execution of search warrants at the defendants' residences, the above process was followed to the extent not prevented by encryption-related technology. These devices are identified in the reports of examination related to the devices seized from defendants Good, Spearman, Garrell, and Boyles that the government has produced in discovery.

The Forensic Examination of Digital Devices

In addition to testifying that reliable forensic tools were used to extract, parse, and examine data from the defendants' digital devices, Mr. Marsh is also expected to testify about the results of the forensic examination of these devices. In this sense, Mr. Marsh will be testifying more in the nature of a fact witness, explaining how he was able to locate and preserve certain evidence from the forensic image copies of the devices he examined. Nevertheless, out of an abundance of caution, the United States is also providing notice that it intends to offer testimony from Mr. Marsh regarding the results of the forensic examinations of the seized devices referenced above, including but not limited to the following:

- With respect to defendant Gregory Malcolm Good:
    - Q-HQ-002 – a 32 GB ONN USB thumb drive (S/N: 90000119142C5432);
    - Q-HQ-003 – a Sandisk 32 GB USB thumb drive (S/N: 04020002120120013621);
    - Q-HQ-005 – a Sandisk 64 GB USB thumb drive (S/N: 04017021092021090609); and
    - Q-HQ-008 – an HP Pavilion desktop computer (S/N: 8CG008044Z) containing one Toshiba 1 TB hard disk drive ("HDD") (S/N: Y9G1KE7MSFWC);
- With respect to defendant William Michael Spearman:

- 1B32 – a Lenovo ThinkPad (S/N: PC0DTEGP);
- 1B34 – an HGST HDD (S/N: Y1GE9Y6L);
- 1B35 – a Getac S400 laptop (S/N: RC439S0359) containing one HDD;
- 1B41 – a Strantium thumb drive (S/N: AACM2W3BQC12UKXL);
- 1B42 – a Seagate external HDD (S/N: NABR6R52);
- 1B45 – a Seagate external HDD (S/N: NABR6R4T);
- 1B48 – a Toshiba Satellite Laptop (S/N: XC301289R) containing one optical disc and one solid state drive; and
- 1B49 – a PNY thumb drive (S/N: 097902B88050);

- With respect to defendant Matthew Branden Garrell:
  - 1B51 – a Sandisk 64 GB USB thumb drive (S/N: BN2Q085Y012W); and
  - 1B53 – a Sandisk 64 GB USB thumb drive (S/N: BN2203001114W); and
- With respect to defendant Robert Preston Boyles:
  - 1B56 – an HP Pavilion laptop (S/N: 8CG0191TQV); and
  - 1B57 – a Sandisk Cruzer Glide 16 GB USB drive (S/N: 4C530000110413115272).

The results of the forensic examination of these digital devices have been produced to the defendants in discovery in form of the above-referenced reports of examination.[2] Accordingly, pursuant to Fed. R. Crim. P. 16(a)(1)(F) & (G)(iv), the results of the forensic examination of these devices will not be repeated in full here. Generally speaking, however, Mr. Marsh may testify as to how the above devices contained child pornography, evidence related to the accessing or operation of Website A and evidence tying the use and ownership of a particular device to a

[2] Consistent with 18 U.S.C. § 3509(m) and the Protective Orders the Court entered in this matter, the United States has made and will continue to make the contraband evidence recovered through the forensic examination of these devices reasonably available to the defense at an appropriate government facility.

specific defendant. Mr. Marsh may also testify as to how some of these devices could not be forensically examined due to user-enabled encryption.

The Analysis of Computer Server Data

In addition to the above, Mr. Marsh is expected to testify about his ability to parse and analyze data obtained from computer servers that host and run websites. In particular, Mr. Marsh may testify that websites are run via computer servers that may be hosted either by an individual at a residence or at a business such as a hosting company that maintains computers, which may be physical or virtual, connected to the internet. Mr. Marsh may further testify as to how an individual who operates a computer server running a website is able to place files, software code, databases, and other data on the website's server, and he may explain how that server will use those files, software code, databases, and other data to respond to request from Internet users for pages or other resources from the website run via the server. Mr. Marsh may also testify that a computer server hosting a website will store information and logs related to the accessing and operation of the particular website.

Mr. Marsh is further expected to testify that computer forensic examiners are able to create an exact, logical copy of a computer server hosting a website for purposes of examining the contents and data contained on that server, similar to the process described above for digital devices. Mr. Marsh may testify that such servers may contain various files, software codes, databases, and other data related to the website, as described above. Mr. Marsh may then testify that, depending on the nature of the website hosted and run via the server, these database files recoverable from the website's server may include data related to the contents of private messages and emails that were exchanged through the website. Mr. Marsh may explain that a forensic examiner can identify and extract such a database related to email messages exchanged via a website from a logical copy of the computer server and use forensic tools to mount—or display—the contents of that database file in a readable format. Mr. Marsh may further testify that, in the context of a database file related to a private email system utilized by users of a website that is recovered from the website's server, the above process would allow him to open, view, and export all user email content that is recovered from the server. In addition, it is expected that Mr. Marsh will testify as to how the above process was followed with respect to a computer server that hosted Website A to review the contents of email messages exchanged by users of the site.

In accordance with Fed. R. Crim. P.
16(a)(1)(G)(v), I approve this disclosure:

____
JON-ROBERT MARSH
Data Scientist
Federal Bureau of Investigation

b. Joshua Storey

Mr. Storey is a Digital Investigative Analyst ("DIA") in the High Technology Investigative Unit ("HTIU") at the U.S. Department of Justice, Criminal Division, Child Exploitation and Obscenity Section. He has held this position since 2014. In his capacity as a DIA, Mr. Storey conducts forensic analysis of seized computer systems, servers, mobile devices, and other media to provide investigative and analytical support to prosecutors and law enforcement agents. He regularly conducts online investigations and analysis of internet technologies used to commit federal child exploitation offenses. He has conducted and assisted with numerous investigations involving the Tor network and with child pornography offenses involving the Tor network. He has numerous certifications, including certifications in Encase and Cellebrite. In addition to his on-the-job experience analyzing digital devices, he has taken and presented numerous training courses related to the analysis of computers and online child exploitation offenses, including offenses on the Tor network. He holds a bachelor's degree in legal studies and a master's degree in digital forensics from the University of Central Florida. A copy of Mr. Storey's curriculum vitae will be produced in discovery.

In the last four years, Mr. Storey has testified as an expert witness in the following cases: *United States v. Plamen Velinov*, 8:21-CR-00342-VMC-SPF (M.D. Fla. 2023); and *United States v. Willis Pierre Lewis and Brittany Jones*, 1:19-CR-00307-RCL (D.D.C. 2022). He has authored no publications in the last ten years.

The Onion Router Network

The United States may call Mr. Storey to testify about a computer network known as "Tor" (an abbreviation for "The Onion Router"), including its purpose, the way it operates, and the difficulties that it poses for investigators of online criminal activity. In particular, he may contrast the Tor network with the "clearnet," or the ordinary internet. Mr. Storey may testify that the internet is a global network of computers and other devices that are uniquely identified by internet protocol addresses, also known as "IP addresses." Generally, when one device on the internet requests information from a second device, the requesting device identifies its own IP address and communicates it directly to the responding device so that the responding device knows where to send its response. Data transferred over the internet is split into "packets" that contain two parts: a "header" that contains non-content routing and control information, such as a packet's source and destination IP addresses, and a "payload," which generally contains user data or the content of a communication.

Mr. Storey may testify that when individuals commit crimes over the clearnet, law enforcement is frequently available to identify that individual's IP address and then use that information to more specifically identify an offender or a location where the offense took place. For example, if a computer user visits a website in the process of committing a crime, that website frequently records the IP address of the user on a website log. Law enforcement can often then obtain the computer user's IP address from the website, and it can often then determine from an internet service provider certain identifying information associated the internet subscriber that was using that IP address at the time the crime took place. In addition, if a clearnet website itself is facilitating criminal activity, law enforcement can generally determine the IP address of the computer server hosting the website by looking it up on a publicly available Domain Name System ("DNS") listing, which provides information about clearnet websites.

Mr. Storey may also testify that the Tor network is a computer network available to internet users that is designed to facilitate anonymous communication over the internet and to make it more difficult to determine the identity and location of a computer user. The Tor network does this by routing communication through a globally distributed network of relay computers or “nodes,” along a randomly assigned path known as a “circuit.”

Mr. Storey may testify that, to access the Tor network, a user must install Tor software on the user’s device, which is most easily done by downloading the free “Tor Browser” from the Tor Project, which is a private entity that maintains the Tor network. The Tor browser is a web browser that is configured to route a user’s internet traffic through the Tor network. A user may also access and use the Tor network through any computer or electronic device that has been configured to use Tor routing or software, including desktop or laptop computers, smartphones, or tablet computers.

Mr. Storey may further testify that, as with other internet communications, a Tor user’s communications are split into packets that contain header information and a payload and are routed using IP addresses. In order for a Tor user’s communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares his or her IP address with Tor nodes. This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information should be sent to. Those Tor nodes are operated by volunteers—individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

Mr. Storey may testify that Tor may be used to access clearnet websites. Because a Tor user’s communications are routed through multiple nodes before reaching their destination, when a Tor user access such a clearnet website, only the IP address of the last relay computer—known as the “exit node”—appears on that website’s IP address web access log. Put differently, the website can see only the IP address of the computer serving as the exit node, not the computer user’s actual IP address. Accordingly, unlike over the clearnet, law enforcement generally cannot identify or locate a Tor user who has committed a crime over a website by obtaining an IP address from the website's logs, because that IP address will not be the computer user's true, originating IP address. In addition, the contents of a Tor user's communications are encrypted while the communication passes through the Tor network, which prevents the operator of a Tor node from observing the content of other Tor users' communications.

Mr. Storey may further testify that the Tor network makes it possible for users to operate and access websites that are accessible only to users operating over the Tor network and not users operating over the clearnet only. Such websites that are accessible only over the Tor network are called "hidden services" or "onion services," and they are part of what is sometimes referred to as the "dark web." Mr. Storey may testify that these hidden services operate in a manner that attempts to conceal the true IP address of the computer hosting the website. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. Hidden services, however, have unique technical features that attempt to conceal the computer server's location.

Mr. Storey may further testify that, unlike standard internet websites, the web address of a Tor-based hidden service consists of a series of 16 or 56 algorithm-generated characters, followed by the suffix ".onion." Unlike clearnet websites, there is no way to determine the IP address of a computer server that hosts a Tor hidden service through a DNS query. Because of this, while law enforcement can visit, view, and access Tor hidden services that are facilitating illegal activity, they cannot determine the IP address of such a hidden service through public lookups. In addition, as with all Tor communications, communications between Tor users' computers and a Tor hidden service webserver are routed through a series of intermediary computers.

Mr. Storey may further testify that many individuals with an interest in trafficking in child pornography utilize the Tor network for this criminal conduct, that numerous websites dedicated to child pornography have operated over the Tor network, and that the nature and operation of the network has made it difficult for law enforcement to determine the location of the website servers, the identity or location of the individuals behind the website, and the identity or location of the website users.

In accordance with Fed. R. Crim. P. 16(a)(1)(G)(v), I approve this disclosure:

JOSHUA STOREY

Digitally signed by JOSHUA STOREY
Date: 2023.04.12 12:05:05 -04'00'

JOSHUA STOREY
Digital Investigative Analyst
U.S. Department of Justice

c. Scott Schoenhardt

Scott Schoenhardt is a Special Agent ("SA") in the FBI's Child Exploitation Operational Unit, where he is responsible for conducting investigations into and developing technical solutions to address the online sexual exploitation of children. He has served in this role since 2021. From 2017 to 2021, SA Schoenhardt was a Special Agent in the FBI's Cyber Task Force. In that position, he conducted national security investigations and other cyber-related investigations involving violations of federal crimes. Prior to his work at the FBI, SA Schoenhardt worked as a Branch Chief in the U.S. Coast Guard Reserve's Cyber Command.

SA Schoenhardt has extensive experience in conducting digital forensic investigations and analysis on electronic devices, including devices operating on Windows, Mac, and Linux systems. He regularly conducts forensic analysis of seized computers systems, devices, and other digital media to uncover and identify digital artifacts and provide support to other law enforcement agents and prosecutors. Through this work, SA Schoenhardt has developed extensive knowledge of and experience working with forensic tools used to examine digital devices. He also has numerous professional certifications related to digital forensics, including certifications as a forensic analyst, as a forensic examiner, as a digital extraction technician, and in advanced smartphone forensics, among others. In addition to his certifications and his on-the-job experience analyzing digital devices, SA Schoenhardt has taken numerous training courses related to the forensic examination and analysis of digital devices. He also holds a bachelor's degree in Criminal Justice and Political Science from Canisius College and a master's degree in Cybersecurity Concentration in Digital Forensics from Utica University. A copy of SA Schoendhart's curriculum vitae will be produced in discovery.

In the last four years, SA Schoenhardt has not testified as an expert witness at trial or by deposition. In the last ten years, he has authored the following publication: Scott Schoenhardt, Macintosh APFS Forensic Software Assessment: BlackBag Technologies BlackLight 2019 R3 (May 2020) (unpublished M.S. thesis) (on file with Utica University).

The Forensic Examination of Digital Devices

SA Schoenhardt is expected to testify about the FBI's forensic examination of electronic devices that were discovered on-scene and seized during the execution of a warrant to search defendant Spearman's residence in the Northern District of Alabama. As relevant for purposes of this notice, SA Schoenhardt may testify that approximately ten devices seized from Spearman's residence could not be forensically examined because they were encrypted by the user. These devices and the related findings regarding encryption are described more fully in the above-referenced report of examination related to Spearman's devices, which the government has produced in discovery. SA Schoenhardt is further expected to testify about the FBI's efforts to forensically examine a Lenovo laptop, identified in the report of examination as item 1B32 - a Lenovo ThinkPad (S/N: PC0DTEGP), that was recovered and seized during the search of Spearman's residence and photographs of which were produced in discovery. In particular, SA Schoenhardt may testify that the laptop's screen was visible but frozen when the device was discovered during the search, that various other electronic devices had been and/or were connected to that device (including but not limited to a 4 TB drive and a PNY thumb drive), and that various encryption- and Tor-related forensic artifacts were visible on the laptop's screen.

SA Schoenhardt is also expected to testify about device encryption more generally, including by explaining what encryption is and how various encryption-related technologies like Tails and BitLocker operate. In particular, SA Schoenhardt may testify that Tails is a portable, security-focused operating system that may be password protected by a user and that runs from the memory of a computer so as to leave no forensic trace written on the computer's hard disk drive. SA Schoenhardt may also testify that BitLocker is a technology used to encrypt digital devices and explain the process by which a BitLocker-encrypted drive can be accessed using a unique BitLocker recovery key. SA Schoenhardt may also testify as to how evidence of the use of Tails and/or BitLocker was recovered from defendant Spearman's electronic devices, including but not limited to the Lenovo laptop (item 1B32), a Getac laptop (item 1B35), a Toshiba Satellite laptop (item 1B48), and various other devices identified and described more fully in the above-referenced report of examination.

In accordance with Fed. R. Crim. P.
16(a)(1)(G)(v), I approve this disclosure:

SCOTT SCHOENHARDT
Special Agent
Federal Bureau of Investigation

2. Notice of Request for Reciprocal Discovery

With respect to each of the defendants in this matter, the United States requests the following.

Under Rule 16(b)(1)(A), the United States requests to inspect, copy, and photograph any and all books, papers, documents, photographs, tangible objects, or make copies of portions thereof, which are within the possession, custody or control of the defendant and that the defendant intends to introduce as evidence in his case-in-chief at trial.

Under Rule 16(b)(1)(B), the United States requests to inspect and copy or photograph any results or reports of physical or mental examinations and of scientific tests or experiments made in connection with this case, which are in the possession or control of the defendant that he intends to introduce as evidence at the trial or that were prepared by a witness whom the defendant intends to call.

Under Rule 16(b)(1)(C), the United States requests a written statement of any testimony that the defendant intends to use under Rules 702, 703, and/or 705 of the Federal Rules of Evidence as evidence at trial. This statement must include a complete statement of all opinions that the defendant will elicit from the witness in the defendant's case-in-chief; the bases and reasons for them; the witness's qualifications, including a list of all publications authored in the previous 10 years; and, a list of all other cases in which, during the previous 4 years, the witness has testified as an expert at trial or by deposition.

//

//

//

//

The United States also asks for prior statements of all witnesses (except the defendant) under Rule 26.2.

MARKENZY LAPOINTE
UNITED STATES ATTORNEY

By: *s/ Gregory Schiller*
GREGORY SCHILLER
Assistant United States Attorney
Court Id No. A5501906
U.S. Attorney's Office - SDFL
500 S. Australian Ave., Suite 400
West Palm Beach, Florida 33401
Telephone: (561)209-1045
E-mail: gregory.schiller@usdoj.gov

By: *s/Kyle Reynolds*
KYLE REYNOLDS
TRIAL ATTORNEY
U.S. Dept. of Justice, Criminal Division
Child Exploitation and Obscenity Section
Court ID # A5502872
1301 New York Avenue, NW
Washington, DC 20005
Phone: (202) 616-2842
Email: kyle.reynolds@usdoj.gov

By: *s/William G. Clayman*
WILLIAM G. CLAYMAN
TRIAL ATTORNEY
U.S. Dept. of Justice, Criminal Division
Child Exploitation and Obscenity Section
Court ID # A5502958
1301 New York Avenue, NW
Washington, DC 20005
Phone: (202) 514-0040
Email: william.clayman@usdoj.gov

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on April 12, 2023, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF.

s/*William G. Clayman*
William G. Clayman
Trial Attorney